

1 JONATHAN D. MCDOUGALL
STATE BAR NO. 212359
2 1640 Laurel Street
San Carlos, CA 94070
3 Telephone: (650) 594-4200
Facsimile: (650) 594-4205
4

Attorney for Defendant
5 BRYAN HENDERSON

6 UNITED STATES DISTRICT COURT
7 NORTHERN DISTRICT OF CALIFORNIA
8 SAN FRANCISCO DIVISION

9 THE UNITED STATES OF AMERICA,)
10)
Plaintiff,)
11)
vs.)
12)
13 BRYAN HENDERSON,)
14)
Defendant.)
15
16
17
18
19
20
21
22
23
24
25

NO. CR-15-CR-0565-WHO

EXHIBITS A THROUGH D TO
MOTION TO SUPPRESS NIT SEARCH
WARRANT

Date: June 30, 2016
Time: 1:30 p.m.

EXHIBIT A

U.S. V. BRYAN HENDERSON

CR-15-0565-WHO

MOTION TO SUPPRESS NIT

SEARCH WARRANT

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the
Northern District of California

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)The residence located at 1106 E. 16th Avenue,
San Mateo, California 94402

Case No.

3-15-71083

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Northern District of California
(identify the person or describe the property to be searched and give its location):

The residence located at 1106 E. 16th Avenue, San Mateo, California 94402, as described in Attachment A, incorporated herein by reference.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (Identify the person or describe the property to be seized):

Evidence of a crime; contraband, fruits of crime, or other items illegally possessed, and/or property designed for use, intended for use, or used in committing a crime; specifically, knowing, conspiracy to, or attempted access with intent to view child pornography, in violation of Title 18, United States Code, Sections 2252A(a)(5)(B) and (b)(2), as set forth in Attachment B and using the protocol set forth in Attachment C, with Attachments B and C incorporated herein by reference.

YOU ARE COMMANDED to execute this warrant on or before September 8, 2015 (not to exceed 14 days)
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to The Honorable Joseph C. Spero
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for days (not to exceed 30) ☐ until, the facts justifying, the later specific date of

Date and time issued:

8/24/15 3:55 pm

Judge's signature

City and state:

San Francisco, California

Joseph C. Spero, Chief United States Magistrate Judge

Printed name and title

BH-000095

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.: <u>3-15-71083</u>	Date and time warrant executed: <u>9-2-2015 06:25 am</u>	Copy of warrant and inventory left with: <u>Bryan Henderson</u>
--------------------------------	---	--

Inventory made in the presence of:

SA Kelli K. Johnson-FBI

Inventory of the property taken and name of any person(s) seized:

The property seized were multiple electronic devices (40 total) in accordance with Attachment B: laptops, desktop computers, external hard drives, thumb drives, CD's, ipod, tablets, and cell phones.

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 9-3-2015


Executing officer's signature

Kelli K. Johnson-Special Agent, FBI
 Printed name and title

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
Northern District of California

JCS

In the Matter of the Search of
*(Briefly describe the property to be searched
 or identify the person by name and address)*
 The residence located at 1106 E. 16th Avenue,
 San Mateo, California 94402

Case No. **3-15-71083**

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(Identify the person or describe the property to be searched and give its location)*:
 The residence located at 1106 E. 16th Avenue, San Mateo, California 94402, as further described in Attachment A.

located in the Northern District of California, there is now concealed *(Identify the person or describe the property to be seized)*:
 As set forth in Attachment B.

FILED

AUG 24 2015

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

RICHARD W. WIEKING
 CLERK, U.S. DISTRICT COURT
 NORTHERN DISTRICT OF CALIFORNIA

SEALED
BY COURT ORDER

The search is related to a violation of:

Code Section	Offense Description
21 USC 2252A(a)(5)(B), (b)(2)	Knowing, conspiracy to, or attempted access with intent to view child pornography

The application is based on these facts:
 As set forth in the attached affidavit of Special Agent Kelli K. Johnson.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Approved as to form
Sheila A.G. Armbrust
 AUSA Sheila A.G. Armbrust

Kelli K. Johnson
(Applicant's signature)
 Kelli K. Johnson, Special Agent, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 6/25/15City and state: San Francisco, California

Joseph C. Spero
Judge's signature
 Joseph C. Spero, Chief United States Magistrate Judge
Printed name and title

BH-000097

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Kelli K. Johnson, being first duly sworn, hereby depose and state as follows:

I. Introduction and Qualifications of Affiant

1. I have been employed as a Special Agent of the FBI since September 2012 and am currently assigned to the San Francisco Field Office, Oakland Resident Agency in a squad that investigates crimes against children. Prior to my service with the FBI, I was a commercial airline pilot. From my employment as an the FBI Special Agent, I have investigated, among other things, federal criminal violations related to cybercrime, child pornography, and the sexual exploitation of minors. I am currently assigned to investigate cases involving the sexual exploitation of minors, including such exploitation via the Internet and computers. As an FBI agent, I am authorized to investigate violations of federal law and execute warrants issued under the authority of the United States. I have received training and possess experience relating to federal criminal procedures and federal statutes. I have also received specialized training and instruction in the field of sexual exploitation of minors, to include child and adolescent forensic interviewing. I have experience investigating violations of child pornography and child exploitation and have reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251 and 2252A, and I am authorized by the Attorney General to request a search warrant.

2. I respectfully submit this Application and Affidavit in support of a warrant authorizing a search of the premises known and described as 1106 E. 16th Avenue, San Mateo, California 94402 (the "SUBJECT PREMISES"), which is located in the Northern District of California. The SUBJECT PREMISES is further described in Attachments A and B, which are incorporated by reference herein. For the reasons stated below, I submit that there is probable cause to believe that the SUBJECT PREMISES presently contains evidence of a crime, fruits of a crime, and instrumentalities of violations of 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) (possession of, knowing access, conspiracy to access, or attempted access with intent to view child pornography).

3. Located within the SUBJECT PREMISES to be searched, I seek to seize evidence, fruits, and instrumentalities of the foregoing criminal violations. I request authority to search the entire SUBJECT PREMISES, including the residential dwelling and any computer and computer media located therein where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as contraband and instrumentalities, fruits, and evidence of crime.

4. The statements contained in this affidavit are based in part on: information provided by FBI Special Agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents, information gathered from the service of administrative subpoenas; the results of physical and electronic surveillance conducted by law enforcement agents; independent investigation and analysis by FBI agents/analysts and computer forensic professionals; and my experience, training and background as a Special Agent (SA) with the FBI. Because this affidavit is being submitted for

the limited purpose of securing authorization for the requested warrant to search the SUBJECT PREMISES, I have not included each and every fact known to me concerning this investigation. Instead, I have set forth only the facts that I believe are necessary to establish the necessary foundation for the requested warrant.

II. Description of the SUBJECT PREMISES

5. The SUBJECT PREMISES is described as a cream colored single-story, single family residence with an attached garage. The numbers 1106 are affixed to the front of the residence adjacent to the door of the garage. (See Attachment A.)

III. Relevant Statute

6. This investigation concerns alleged violations of 18 U.S.C. § 2252A(a)(5)(B) and (b)(2), Possession and Access, or Attempted Access, with Intent to View Child Pornography.

7. 18 U.S.C. § 2252A(a)(5)(B) and (b)(2) prohibits a person from knowingly possessing or knowingly accessing with intent to view, or attempting to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

IV. Definitions

8. The following definitions apply to this Affidavit and attachments hereto:

a. "Bulletin Board" means an Internet-based website that is either secured (accessible with a password) or unsecured, and provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as "internet forums" or "message boards." A "post" or "posting" is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message "thread," often labeled a "topic," refers to a linked series of posts and reply messages. Message threads or topics often contain a title, which is generally selected by the user who posted the first message of the thread. Bulletin boards often also provide the ability for members to communicate on a one-to-one basis through "private messages." Private messages are similar to e-mail messages that are sent between two members of a bulletin board. They are accessible only by the user who sent/received such a message, or by the Website Administrator.

b. "Chat" refers to any kind of communication over the Internet that offers a real-time transmission of text messages from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

c. **"Child Erotica"** means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, legally obscene or that do not necessarily depict minors in sexually explicit conduct.

d. **"Child Pornography"** is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

e. **"Computer"** is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

f. **"Computer Server" or "Server"** is a computer that is attached to a dedicated network and serves many users. A web server, for example, is a computer which hosts the data associated with a website. That web server receives requests from a user and delivers information from the server to the user's computer via the Internet. A domain name system ("DNS") server, in essence, is a computer on the Internet that routes communications when a user types a domain name, such as www.cnn.com, into his or her web browser. Essentially, the domain name must be translated into an Internet Protocol ("IP") address so the computer hosting the web site may be located, and the DNS server provides this function.

g. **"Computer hardware"** consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

h. **"Computer software"** is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

i. **"Computer-related documentation"** consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

j. "Computer passwords, pass-phrases and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

k. "File Transfer Protocol" ("FTP") is a standard network protocol used to transfer computer files from one host to another over a computer network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server.

l. "Host Name" is a name assigned to a device connected to a computer network that is used to identify the device in various forms of electronic communication, such as communications over the Internet;

m. "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

n. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

o. "Internet Service Providers" ("ISPs") are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line ("DSL") or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an Internet Service Provider ("ISP") over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

p. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.

q. Media Access Control ("MAC") address: The equipment that connects a computer to a network is commonly referred to as a network adapter. Most network adapters have a MAC address assigned by the manufacturer of the adapter that is designed to be a unique identifying number. A unique MAC address allows for proper routing of communications on a network. Because the MAC address does not change and is intended to be unique, a MAC address can allow law enforcement to identify whether communications sent or received at different times are associated with the same adapter.

r. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

s. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

t. "Secure Shell" ("SSH") is a security protocol for logging into a remote server. SSH provides an encrypted session for transferring files and executing server programs.

u. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

v. "URL" is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or

typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

w. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

x. "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language ("HTML") and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol ("HTTP");

V. Probable Cause

9. A user of the Internet account at 1106 E. 16th Avenue, San Mateo, CA 94402 has been linked to an online community of individuals who regularly send and receive child pornography via a website that operated on an anonymous online network. The website is described below and referred to herein as "Website A."¹ There is probable cause to believe that Bryan Henderson or a user of the Internet account at the SUBJECT PREMISES knowingly accessed with intent to view child pornography on "Website A."

A. The Network²

10. "Website A" operated on a network ("the Network") available to Internet users who are aware of its existence. The Network is designed specifically to facilitate anonymous communication over the Internet. In order to access the Network, a user must install computer software that is publicly available, either by downloading software to the user's existing web browser, downloading free software available from the Network's administrators, or

¹ Law enforcement knows the actual name of "Website A," but disclosure of the name of the site would potentially alert its members to the fact that law enforcement action is being taken against the site and its users, potentially provoking members to notify other members of law enforcement action, flee, and/or destroy evidence. Accordingly, for purposes of the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the website will be identified as "Website A."

² Law enforcement knows the actual name of the Network. The Network remains active and disclosure of the name of the Network would potentially alert its members to the fact that law enforcement action is being taken against the network, potentially provoking members to notify other members of law enforcement action, flee, and/or destroy evidence. Accordingly, for purposes of the confidentiality and integrity of the ongoing investigation involved in this matter, specific names and other identifying factors have been replaced with generic terms and the network will be identified as "the Network."

downloading a publicly-available third-party application.³ Using the Network prevents someone attempting to monitor an Internet connection from learning what sites a user visits and prevents the sites the user visits from learning the user's physical location. Because of the way the Network routes communication through other computers, traditional IP identification techniques are not viable.

11. Websites that are accessible only to users within the Network can be set up within the Network and "Website A" was one such website. Accordingly, "Website A" could not generally be accessed through the traditional Internet.⁴ Only a user who had installed the appropriate software on the user's computer could access "Website A." Even after connecting to the Network, however, a user had to know the exact web address of "Website A" in order to access it. Websites on the Network are not indexed in the same way as websites on the traditional Internet. Accordingly, unlike on the traditional Internet, a user could not simply perform a Google search for the name of "Website A," obtain the web address for "Website A," and click on a link to navigate to "Website A." Rather, a user had to have obtained the web address for "Website A" directly from another source, such as other users of "Website A," or from online postings describing both the sort of content available on "Website A" and its location. Accessing "Website A" therefore required numerous affirmative steps by the user, making it extremely unlikely that any user could have simply stumbled upon "Website A" without first understanding its content and knowing that its primary purpose was to advertise and distribute child pornography.

12. The Network's software protects users' privacy online by bouncing their communications around a distributed network of relay computers run by volunteers all around the world.

13. The Network also makes it possible for users to hide their locations while offering various kinds of services, such as web publishing, forum/website hosting, or an instant messaging server. Within the Network itself, entire websites can be set up which operate the same as regular public websites with one critical exception - the IP address for the web server is hidden and instead is replaced with a Network-based web address. A user can only reach such sites if the user is using the Network client and operating in the Network. Because neither a user nor law enforcement can identify the actual IP address of the web server, it is not possible to determine through public lookups where the computer that hosts the website is located. Accordingly, it is not possible to obtain data detailing the activities of the users from the website server through public lookups.

³ Users may also access the Network through so-called "gateways" on the open Internet, however, use of those gateways does not provide users with the full anonymizing benefits of the Network.

⁴ Due to a misconfiguration, prior to February 20, 2015, "Website A" occasionally was accessible through the traditional Internet. In order to access "Website A" in that manner, however, a user would have had to know the exact IP address of the computer server that hosted "Website A," which information was not publicly available. As of on or about February 20, 2015, "Website A" was no longer accessible through the traditional Internet.

B. Description of "Website A" and Its Content

14. Based on the investigation of other FBI agents, I know that "Website A" was a child pornography bulletin board and website dedicated to the advertisement and distribution of child pornography and the discussion of matters pertinent to the sexual abuse of children, including the safety and security of individuals who seek to sexually exploit children online. On or about February 20, 2015, the computer server hosting "Website A" was seized from a web-hosting facility in Lenoir, North Carolina. "Website A" operated in Newington, Virginia, from February 20, 2015, until March 4, 2015, at which time "Website A" ceased to operate. Between February 20, 2015, and March 4, 2015, law enforcement agents acting pursuant to an order of the United States District Court for the Eastern District of Virginia monitored electronic communications of users of "Website A." Before, during, and after its seizure by law enforcement, law enforcement agents viewed, examined and documented the contents of "Website A," which are described below.

15. According to statistics posted on the site, "Website A" contained a total of 117,773 posts, 10,622 total topics, and 214,898 total members as of March 4, 2015. The website appeared to have been operating since approximately August 2014, which is when the first post was made on the message board. On the main page of the site, located to either side of the site name were two images depicting partially clothed prepubescent girls with their legs spread apart, along with the text underneath stating, "No cross-board reposts, .7z preferred, encrypt filenames, include preview, Peace out." Based on my training and experience, I know that "no cross-board reposts" refers to a prohibition against material that is posted on other websites from being "re-posted" to "Website A," and ".7z" refers to a preferred method of compressing large files or sets of files for distribution. Two data-entry fields with a corresponding "Login" button were located to the right of the site name. Located below the aforementioned items was the message, "Warning! Only registered members are allowed to access the section. Please login below or 'register an account' [(a hyperlink to the registration page)] with "[Website A]." Below this message was the "Login" section, consisting of four data-entry fields with the corresponding text, "Username, Password, Minutes to stay logged in, and Always stay logged in."

16. Upon accessing the "register an account" hyperlink, there was a message that informed users that the forum required new users to enter an email address that looks to be valid. However, the message instructed members not to enter a real email address. The message further stated that once a user registered (by selecting a user name and password), the user would be able to fill out a detailed profile. The message went on to warn the user "[F]or your security you should not post information here that can be used to identify you." The message further detailed rules for the forum and provided other recommendations on how to hide the user's identity for the user's own security.

17. After accepting the above terms, registration to the message board then required a user to enter a username, password, and e-mail account; although a valid e-mail account was not required as described above.

18. After successfully registering and logging into the site, the user could access any number of sections, forums, and sub-forums. Some of the sections, forums, and sub-forums available to users included: (a) How to; (b) General Discussion; (c) [Website A] information and

rules; and (d) Security & Technology discussion. Additional sections, forums, and sub-forums included (a) Jailbait – Boy; (b) Jailbait – Girl; (c) Preteen – Boy; (d) Preteen – Girl; (e) Pre-teen Videos – Girl HC; (f) Pre-teen Videos – Boys HC; (g) Toddlers; and (h) Kinky Fetish – Scat. Based on my training and experience, I know that “jailbait” refers to underage but post-pubescent minors; the abbreviation “HC” means hardcore (i.e., depictions of penetrative sexually explicit conduct); and “scat” refers to the use of feces in various sexual acts, watching someone defecating, or simply seeing the feces. An additional section and forum was also listed in which members could exchange usernames on a Network-based instant messaging service that I know, based upon my training and experience, to be commonly used by subjects engaged in the online sexual exploitation of children.

19. A review of the various topics within the above forums revealed each topic contained a title, the author, the number of replies, the number of views, and the last post. The “last post” section of a particular topic included the date and time of the most recent posting to that thread as well as the author. Upon accessing a topic, the original post appeared at the top of the page, with any corresponding replies to the original post included in the post thread below it. Typical posts appeared to contain text, images, thumbnail-sized previews of images, compressed files (such as Roshal Archive files, commonly referred to as “.rar” files, which are used to store and distribute multiple files within a single file), links to external sites, or replies to previous posts.

20. A review of the various topics within the “[Website A] information and rules,” “How to,” “General Discussion,” and “Security & Technology discussion” forums revealed that the majority contained general information in regards to the site, instructions and rules for how to post, and welcome messages between users.

21. A review of topics within the remaining forums revealed the majority contained discussions about, and numerous images that appeared to depict, child pornography and child erotica depicting prepubescent girls, boys, and toddlers. Examples of these are as follows:

a. On February 3, 2015, a user posted a topic entitled “Buratino-06” in the forum “Pre-teen – Videos - Girls HC” that contained numerous images depicting child pornography of a prepubescent or early pubescent girl. One of these images depicted the girl being orally penetrated by the penis of a naked male;

b. On January 30, 2015, a user posted a topic entitled “Sammy” in the forum “Pre-teen – Photos – Girls” that contained hundreds of images depicting child pornography of a prepubescent girl. One of these images depicted the female being orally penetrated by the penis of a male; and

c. On September 16, 2014, a user posted a topic entitled “9yo Niece - Horse.mpg” in the “Pre-teen Videos - Girls HC” forum that contained four images depicting child pornography of a prepubescent girl and a hyperlink to an external website that contained a video file depicting what appeared to be the same prepubescent girl. Among other things, the video depicted the prepubescent female, who was naked from the waist down with her vagina and anus exposed, lying or sitting on top of a naked adult male, whose penis was penetrating her anus.

22. A list of members, which was accessible after registering for an account, revealed that approximately 100 users made at least 100 posts to one or more of the forums. Approximately 31 of these users made at least 300 posts. In total, "Website A" contained thousands of postings and messages containing child pornography images. Those images included depictions of nude prepubescent minors lasciviously exposing their genitals or engaged in sexually explicit conduct with adults or other children.

23. "Website A" also included a feature referred to as "[Website A] Image Hosting." This feature of "Website A" allowed users of "Website A" to upload links to images of child pornography that are accessible to all registered users of "Website A." On February 12, 2015, an FBI Agent accessed a post on "Website A" titled "Giselita" which was created by a particular "Website A" user. The post contained links to images stored on "[Website A] Image Hosting." The images depicted a prepubescent girl in various states of undress. Some images were focused on the nude genitals of a prepubescent girl. Some images depicted an adult male's penis partially penetrating the vagina of a prepubescent girl.

24. Text sections of "Website A" provided forums for discussion of methods and tactics to use to perpetrate child sexual abuse. For example, on January 8, 2015, a user posted a topic entitled "should i proceed?" in the forum "Stories - Non-Fiction" that contained a detailed accounting of an alleged encounter between the user and a 5 year old girl. The user wrote "... it felt amazing feeling her hand touch my dick even if it was through blankets and my pajama bottoms..." The user ended his post with the question, "should I try to proceed?" and further stated that the girl "seemed really interested and was smiling a lot when she felt my cock." A different user replied to the post and stated, "... let her see the bulge or even let her feel you up...you don't know how she might react, at this stage it has to be very playful..."

C. Court Authorized Use of Network Investigative Technique

25. Based on my training and experience, I know that websites generally have Internet Protocol ("IP") address logs that can be used to locate and identify the site's users. In such cases, after the seizure of a website whose users were engaging in unlawful activity, law enforcement could review those logs in order to determine the IP addresses used by users of "Website A" to access the site. A publicly available lookup could then be performed to determine what Internet Service Provider ("ISP") owned the target IP address. A subpoena could then be sent to that ISP to determine the user to which the IP address was assigned at a given date and time.

26. However, because of the Network software utilized by "Website A," any such logs of user activity would contain only the IP addresses of the last computer through which the communications of "Website A" users were routed before the communications reached their destinations. The last computer is not the actual user who sent the communication or request for information, and it is not possible to trace such communications back through the Network to that actual user. Such IP address logs therefore could not be used to locate and identify users of "Website A."

27. Accordingly, on February 20, 2015, the same date "Website A" was seized, the United States District Court for the Eastern District of Virginia authorized a search warrant to

allow law enforcement agents to deploy a Network Investigative Technique ("NIT") on "Website A" in an attempt to identify the actual IP addresses and other identifying information of computers used to access "Website A." Pursuant to that authorization, between February 20, 2015, and approximately March 4, 2015, each time any user or administrator logged into "Website A" by entering a username and password, the FBI was authorized to deploy the NIT which would send one or more communications to the user's computer. Those communications were designed to cause the receiving computer to deliver to a computer known to or controlled by the government data that would help identify the computer, its location, other information about the computer, and the user of the computer accessing "Website A." That data included: the computer's actual IP address, and the date and time that the NIT determined what that IP address was; a unique identifier generated by the NIT (e.g., a series of numbers, letters, and/or special characters) to distinguish the data from that of other computers; the type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86); information about whether the NIT had already been delivered to the computer; the computer's Host Name; the computer's active operating system username; and the computer's MAC address.

D. User "askjeff" On "Website A"

28. According to data obtained from logs on "Website A," monitoring by law enforcement, and the deployment of a NIT, a user with the user name "askjeff" engaged in the following activity on "Website A."

29. The profile page of user "askjeff" indicates this user originally registered an account on "Website A" on or about September 9, 2014. Profile information on "Website A" may include contact information and other information that is supplied by the user. It also contains information about that user's participation on the site, including statistical information about the user's posts to the site and a categorization of those posts. According to the profile for the user "askjeff", this user was a "Newbie" Member of "Website A." Further, according to the Statistics section of this user's profile, the user "askjeff" had been actively logged into the website for a total of 32 hours, 33 minutes and 22 seconds between the dates of September 9, 2014 and March 1, 2015.

30. According to data obtained from logs on "Website A," monitoring by law enforcement, and the deployment of a NIT, on March 1, 2015 at 03:43 UTC, the user "askjeff" engaged in the following activity on "Website A" from IP address 67.188.155.166. During the session described below, the user "askjeff" browsed "Website A" after logging into "Website A" with a username and a password.

31. On March 1, 2015 at 03:43 UTC, the user "askjeff" with IP address 67.188.155.166 accessed the post titled "Two girls with a cam". I reviewed this post, which contained links to the full files and the following text (among other text) "Here are some videos made by this [sic] two girls...In the last ones, there are some lesbian actions". Below the links, the original poster provided a password to download and view the files. In further reviewing this post, I saw that another user of "Website A" posted several comments within a reply thread of the post, which included the message "Girls HC/Re: sex sex sex ... what's this gay stuff doing in a preteen girls section?". Based on the nature of "Website A," the reference to "two girls," the

comment within the original post, and the comments in reply to the post, I believe the file "Two girls with a cam" likely contained child pornography.

32. During the following additional sessions, the user "askjeff" browsed "Website A" after logging into "Website A" with a username and password. During these sessions, IP address information was not collected.

33. On or about February 27, 2015, the user "askjeff" accessed a post that contained a link to a compilation of images that depict child pornography. The post was titled "Two cute girls yelp as they get the tip of a dick." and the post was contained in the forum "Girls HC". I reviewed the images that were displayed as previews in the original post, and I verified that they are child pornography. Specifically, the images show two naked pre-pubescent girls lying on their backs horizontally, one atop the other. Twelve of the images lasciviously display the vaginas of the pre-pubescent girls. In at least six of the photos, an adult male penis is being inserted into each pre-pubescent girl's vagina.

34. On or about February 21, 2015, the user "askjeff" accessed a post within the forum "Girls HC" that contained a link to a compilation of images that depict child pornography. I reviewed the images that were displayed as previews in the original post, and I verified that they are child pornography. Specifically, the images show a pre-pubescent girl performing oral sex on an adult male.

E. IP Address and Identification of User "askjeff" on "Website A"

35. Using publicly available websites, FBI Special Agents were able to determine IP Address 67.188.155.166 was operated by the Internet Service Provider ("ISP") Comcast.

36. In March 2015, an administrative subpoena/summons was served to Comcast requesting information related to the user who was assigned to the aforementioned IP address. According to information received from Comcast, Elizabeth Henderson has been the Internet service subscriber at the SUBJECT PREMISES since June 30, 2003. Internet service was current as of March 13, 2015 at the SUBJECT PREMISES.

37. I performed a search of the Accurant information database (a public records database that provides names, dates of birth, addresses, associates, telephone numbers, email addresses, etc.) for 1106 E. 16th Avenue, San Mateo, CA 94402. According to these public records, Elizabeth Henderson's current address is 1106 E. 16th Avenue, San Mateo, CA 94402 and possible residents of the SUBJECT PREMISES include Bryan Henderson and Matthew Henderson.

38. Among the information collected by the NIT when it was deployed against "askjeff" was the computer's Host Name "KALUMAN-PC" and the computer's Logon Name "kaluman". The same username "kaluman" has a profile and homepage on the publicly available website, "rungs.net". I viewed the publicly available homepage for "kaluman" and observed that the registered name associated with the "kaluman" profile is Bryan Henderson. The webpage indicates the user "kaluman" has been a member since February 15, 2010, is associated with the city of San Mateo, and has a year of birth of 1980.

39. On or about June 8, 2015, FBI SA Robert Basanez requested a query for Bryan Henderson from the California Department of Motor Vehicles (DMV) database. According to the California DMV database, an individual named Bryan Henderson currently resides at the SUBJECT PREMISES. The California DMV records list Bryan Henderson's date of birth as June 8, 1980, which corresponds to the same year of birth as Bryan Henderson "kaluman" profile. Furthermore, the SUBJECT PREMISES is located in San Mateo, which is the same city associated with the Bryan Henderson "kaluman" profile on the website "rungps.net."

40. On or about June 16, 2015, I conducted physical surveillance at the SUBJECT PREMISES. I observed a gray Kia sedan, California license plate 6SPJ246, parked in front of the residence. The results of a California DMV records query indicated the vehicle was registered to Matthew Henderson.

41. On or about June 16 and June 18, 2015, I performed physical surveillance at the SUBJECT PREMISES. I observed a dark colored Acura SUV, California license plate number 5BBB411, parked in the driveway on both occasions. The results of a California DMV records query indicated the vehicle was registered to Gilbert or Barbara Henderson.

42. On or about June 16 and June 18, 2015, I conducted physical surveillance at the SUBJECT PREMISES. I observed a blue Mitsubishi sedan, California license plate number 4YUF852, parked in front of the residence on both occasions. The results of a California DMV records query indicated the vehicle was registered to Gilbert or Barbara Henderson.

43. On or about August 10, 2015, I received information from a representative of the United States Postal Service (USPS) Delivery Unit that services the SUBJECT PREMISES. USPS personnel indicated that Bryan Henderson, Matthew Henderson, and Gilbert Henderson receive mail at the SUBJECT PREMISES.

44. On or about June 18, 2015, I performed a scan of wireless networks (WiFi) available in the vicinity of the SUBJECT PREMISES and observed all WiFi networks were secured, except for one Xfinity WiFi hotspot. Based on my training and experience, I know that any secure WiFi network requires a password to access the Internet. According to Comcast Xfinity's website, wireless gateways provided by Comcast Xfinity broadcast an additional Xfinity network signal, called a "hotspot." This creates an extension of the network in a subscriber's home that any Xfinity subscriber can use to log in and connect to the Internet. However, the secured home WiFi network is completely independent of the Xfinity hotspot. Moreover, any user utilizing the Xfinity hotspot is assigned a different IP address than the IP address that is assigned to the secured home WiFi network. Therefore, the IP address 67.188.155.166 (which was used on March 1, 2015 at 03:43 UTC to connect to "Website A") was specifically only assigned to the SUBJECT PREMISES. Since all WiFi networks available in the vicinity of the SUBJECT PREMISES were password-protected, I believe that an individual utilizing the Internet at the SUBJECT PREMISES would have required a password to access the Internet connection associated with IP address 67.188.155.166 on March 1, 2015 at 03:43 UTC and log onto "Website A".

VI. Characteristics Common to Individuals Who Access with Intent to View Child Pornography

45. Based on my previous investigative experience related to child pornography investigations, as well as the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who utilize web based bulletin boards to access with intent to view images of child pornography:

a. Individuals who access with intent to view child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Individuals who access with intent to view child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who access with intent to view child pornography almost always possess and maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who access with intent to view pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence or inside the collector's vehicle, to enable the individual to view the collection, which is valued highly.

e. Individuals who access with intent to view child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals who would have knowledge about how to access a hidden and embedded bulletin board would have gained knowledge of its location through online communication with others of similar interest. Other forums, such as bulletin boards, newsgroups, IRC chat or chat rooms have forums dedicated to the trafficking of child pornography images. Individuals who utilize these types of forums are considered more advanced users and therefore more experienced in acquiring a collection of child pornography images.

g. Individuals who access with intent to view child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

46. Based on the facts set forth in the paragraphs above, I believe that a user of the Internet account at the SUBJECT PREMISES likely displays characteristics common to individuals who access with the intent to view child pornography.

VII. Background on Computers and Child Pornography

47. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

48. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.

49. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

50. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-Terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files onto them). Media storage devices can easily be concealed and carried on an individual's person.

51. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

52. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer or external media in most cases.

53. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

54. I am familiar with the protocol set forth in Attachment C and will abide by the requirements.

VIII. Search Methodology to be Employed Regarding Electronic Data

55. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- a. on-site triage of computer systems to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, a preliminary scan of image files contained on such systems and digital storage devices

to help identify any other relevant evidence or potential victims, and a scan for encryption software;

b. on-site forensic imaging of any computers that may be partially or fully encrypted, in order to preserve unencrypted electronic data that may, if not immediately imaged on-scene, become encrypted and accordingly unavailable for examination; such imaging may require several hours to complete and require law enforcement agents to secure the search scene until that imaging can be completed;

c. examination of all of the data contained in such computer hardware, computer software, or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

d. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

e. surveying various file directories and the individual files they contain;

f. opening files in order to determine their contents;

g. scanning storage areas;

h. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and

i. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.


IX. Request for Sealing

56. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into a criminal organization and not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness. Further, this affidavit describes a law enforcement technique in sufficient detail that disclosure of this technique could assist others in thwarting its use in the future.

X. Conclusion

57. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B of this Affidavit, are located at the SUBJECT PREMISES, described in Attachment A. I respectfully request that this Court issue a search warrant for the SUBJECT PREMISES, authorizing the seizure and search of the items described in Attachment B.

58. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.


Special Agent Kelli K. Johnson
Federal Bureau of Investigation

Subscribed and sworn to before me this 24th day of August, 2015.

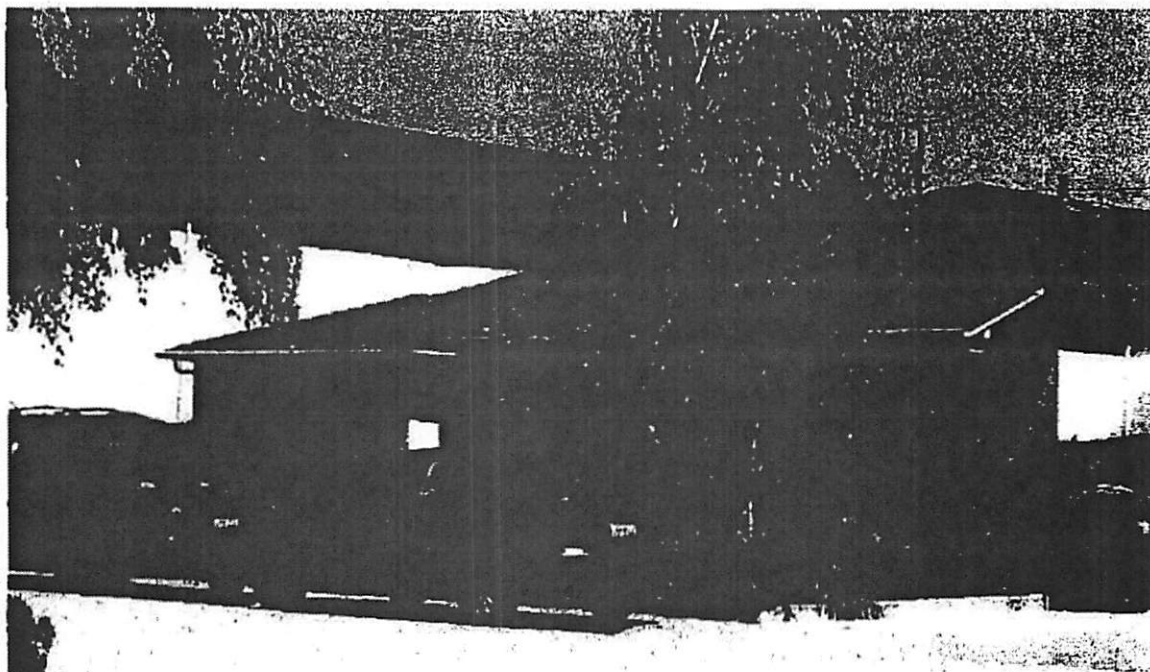

HONORABLE JOSEPH C. SPERO
Chief United States Magistrate Judge

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

The location known as 1106 E. 16th Avenue, San Mateo, CA 94402 is identified as a cream colored single-story, single family residence with an attached garage. The numbers 1106 are affixed to the front of the residence adjacent to the door of the garage.

The premises to be searched includes any appurtenances to the real property that is the SUBJECT PREMISES of 1106 E. 16th Avenue, San Mateo, CA 94402 and any storage units/outbuildings.



ATTACHMENT B

INFORMATION TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Section 2252A:

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;
 - d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
 - e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;
 - f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
 - g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
 - h. evidence of the times the COMPUTER was used;
 - i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
 - k. records of or information about Internet Protocol addresses used by the COMPUTER;
 - l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
 - m. contextual information necessary to understand the evidence described in this attachment.
- 3. Routers, modems, and network equipment used to connect computers to the Internet.
 - 4. Child pornography and child erotica.
 - 5. Records, information, and items relating to violations of the statutes described above including
 - a. Records, information, and items relating to the occupancy or ownership of 1106 E. 16th Avenue, San Mateo, CA 94402 including utility and telephone bills, mail envelopes, or addressed correspondence; Records, information, and items relating to the ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes;
 - b. Records and information relating to the identity or location of the persons suspected of violating the statutes described above; and
 - c. Records and information relating to sexual exploitation of children, including correspondence and communications between users of Website A.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

ATTACHMENT C

December 10, 2010, United States District Court for the Northern District of California

**PROTOCOL FOR SEARCHING DEVICES OR MEDIA THAT STORE DATA
ELECTRONICALLY**

**THIS PROTOCOL WILL BE ATTACHED TO EACH SEARCH WARRANT THAT
AUTHORIZES A SEARCH OF ANY DEVICE OR MEDIA THAT STORES DATA
ELECTRONICALLY**

1. In executing this warrant, the government will begin by ascertaining whether all or part of a search of a device or media that stores data electronically ("the device") reasonably can be completed at the location listed in the warrant ("the site") within a reasonable time. If the search reasonably can be completed on site, the government will remove the device from the site only if removal is necessary to preserve evidence, or if the item is contraband, a forfeitable instrumentality of the crime, or the fruit of a crime.
2. If the government determines that a search reasonably cannot be completed on site within a reasonable time period, the government must determine whether all or part of the authorized search can be completed by making a mirror image of, or in some other manner duplicating, the contents of the device and then conducting the forensic review of the mirror image or duplication off site. The government will complete a forensic review of that mirror image within 120 days of the execution of the search warrant.
3. In a circumstance where the government determines that a mirror image of the contents of a device cannot be created on site in a reasonable time, the government may seize and retain that device for 60 days in order to make a mirror image of the contents of the device.
4. When the government removes a device from the searched premises it may also remove any equipment or documents ("related equipment or documents") that reasonably appear to be necessary to create a mirror image of the contents of the device or conduct an off-site forensic review of a device.
5. When the government removes a device or related equipment or documents from the site in order to create a mirror image of the device's contents or to conduct an off-site forensic review of the device, the government must file a return with a magistrate judge that identifies with particularity the removed device or related equipment or documents within 14 calendar days of the execution of the search warrant.
6. Within a reasonable period of time, but not to exceed 60 calendar days after completing the forensic review of the device or image, the government must use reasonable efforts to return, delete, or destroy any data outside the scope of the warrant unless the government is otherwise permitted by law to retain such data.
7. The time periods set forth in this protocol may be extended by court order for good cause.

8. In the forensic review of any device or image under this warrant the government must make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, or other electronically-stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files to the extent reasonably practicable.

9. For the purposes of this search protocol, the phrase "to preserve evidence" is meant to encompass reasonable measures to ensure the integrity of information responsive to the warrant and the methods used to locate same.